# SENG 4220
# Software Security Engineering
# MIDTERM EXAM

Department of Engineering
Thompson Rivers University
Instructor: Sina Keshvadi

February 28, 2022
Exam duration: 90 minutes

| Question | Score | Points | SLO# |
|---|---|---|---|
| 01 | | 35 | LO-1 |
| 02 | | 11 | LO-1 |
| 03 | | 18 | LO-2 |
| 04 | | 6 | LO-3 |
| 05 | | 6 | LO-1 |
| 06 | | 24 | LO-5 |
| Total | | 100 | ____ |

This is a CLOSED BOOK exam. Textbooks, notes, laptops, personal digital assistants, tablets, and cellular phones are NOT allowed.

It is a 90 minute exam, with a total of 100 marks. There are 6 questions, and 10 pages (including this cover page). Please read each question carefully, and write your answers legibly in the space provided. You may do the questions in any order you wish, but please USE YOUR TIME WISELY.

When you are finished, please hand in your exam paper and sign out.
Good luck!

Student Name: _____ Score: _____ / 100

## Q1 - Software Security Principles (True/False)

2 1. Alex and Brian are building a password management scheme for TRU Library. Ben tells them that they should store a record of (username, MD5(password)) for each user in the database.
True or False: This design protects against offline password hashing attacks.

(a) True

(b) False

**Solution**: False, for two reasons: MD5 is a weak hash, and the password isn't salted.

2 2. When designing a password management scheme, all security guarantees are lost if the attacker gains access to a table containing salt values.

(a) True

(b) False

**Solution**: False. Salts can be public information - their purpose is to prevent dictionary attacks.

2 3. Bob has public key $PK_B$ and private key $K_B$. Assume that $\{\text{message}\}_{key}$ is a secure digital signature of the message with the key.
True or False: $\{\text{“Bob's public key is } PK_B\text{”}\}_{K_B}$ is a valid certificate on Bob's public key

(a) True

(b) False

**Solution**: False. Certificates are signed by someone else's secret key. Bob cannot endorse his own public key.

2 4. Sam and Megan share a symmetric key $K$ not known to anyone else, and H is a secure (unforgeable) MAC (Message Authentication Codes) scheme. Sam presents the statement M = “Megan owes Sam 100 dollars” and the H(K,M) to a judge.
True or False: The judge can be sure that the message was sent by Megan to Sam.

(a) True

(b) False

**Solution**: False. Sam could have constructed the MAC of the message herself.

2 5. A common approach to communicating securely and quickly is first using symmetric-key cryptography to send a key, then using public-key cryptography to send messages.

(a) True

(b) False

**Solution**: False. First use public-key cryptography (slow) to send a key, then use symmetrickey cryptography (fast) to send messages.

2 6. Alice obtains a copy of a digital certificate for Bob from an untrustworthy source. She trusts the certificate authority (CA) who signed Bob's certificate.
True or False: It is safe for Alice to trust the certificate after she verifies the signature.

(a) True

(b) False

**Solution**: True. Where Alice obtained the certificate from does not matter because a trusted CA has signed it, and Alice verifies the signature. Even if the untrustworthy source tried to tamper with the certificate, they would be unable to produce a valid signature without the CA's private key.

2 7. Storing the hash of the passwords prevents any attacker from learning passwords.

(a) True

(b) False

**Solution**: False. Hashing the password forces the attacker to perform a brute-force attack to learn passwords, but it is still possible for the attacker to learn passwords. For example, the attacker can perform an offline dictionary attack using hash tables.

2 8. A bank vault is protected by a locked door, but thieves break into the vault by entering the apartment upstairs and drilling a hole through the ceiling. This is an example of least privilege.

(a) True

(b) False

**Solution**: False. The thieves were never given any unnecessary privileges by the bank. This is an example of failing to ensure complete mediation (or a system being as safe as its weakest link). The bank failed to check an alternate way to access the bank vault. Fun fact: This is the plot of the *Rififi*, which was banned in several countries because it inspired many copycats to try out the same heist.

2 9. One-time pad encryption and decryption can both be parallelized.

(a) True

(b) False

**Solution**: True. When encrypting or decrypting, each bit is XORed with the corresponding bit in the key independently, with no dependence on any other bits.

2 10. Password hashing algorithms should use slower hashes.

(a) True

(b) False

**Solution**: True. Using a slow hash increases the difficulty of a dictionary attack by a significant constant time factor.

## Q1 - Software Security Principles
## Part 2 - Design Principles

You are presented with a list of security principles and a series of scenarios. For each scenario, choose the security principle that is most applicable and provide a one-paragraph explanation of your choice. It is possible for multiple scenarios to share the same security principle, and there may be security principles that are not relevant to any of the scenarios.

**Design Principles:** {DP1: Economy of mechanism; DP2: Fail-safe defaults; DP3: Complete mediation; DP4: Open design; DP5: Separation of privilege; DP6: Least privilege; DP7: Least common mechanism; DP8: Psychological acceptability; DP9: Time-tested tools; DP10: Evidence production; DP11: remnant removal; DP12: reluctant allocation; DP13: security by design; DP14: security is economics; DP15: Defence in depth; DP16: know your adversary.}

3 11. A private high school has 100 students, who each pay $10,000 in tuition each year. The principal hires a SNEG 4220 alum as a consultant, who discovers that the "My Finances" section of the website, which controls students' tuition, is vulnerable to a brute force attack. The consultant estimates an attacker could rent enough compute power with $20 million to break the system, but tells the principal not to worry because of which security principle?

**Solution**: Security is economics. The website handles $1 million per year; not large enough that an attacker would have an incentive to spend $20 million to steal it.

3 12. Sina accidentally released the real midterm questions with solutions in Moodle! In order to conceal what happened, he quickly re-released the sample midterm with the same file name and didn't mention what had happened in the hope that no one would notice. This is an example of not following which security principle?

**Solution**: Open Design. Don't rely on security through obscurity

3 13. Ajay enjoyes SENG 4220 and decide to stay longer in the lab! Abril have two keys: one access the Lab room and another access a closet full of exam questions. Abril gives away only the keys which access the Lab. Which security principle did she consider?

**Solution**: Least privilege

3 14. To access top-secret SENG 4220 data, you must enter a password that only you know, and Sina must enter a second password that only he knows.

> **Solution**: Separation of privilege. If only one person was malicious, they could not access the top-secret data by themselves. Both people need to work together to access the data. This is separation of privilege.

3 15. Many people lock valuables in a safe in their house in addition to locking the doors of the house.

> **Solution**: Defense in Depth. The situation described requires an adversary to work their way past both of two separate defenses

# Q2 - Software Security Definitions

5 1. Complete the following sentence by inserting the provided keywords:

- (a) attacker
- (b) threat
- (c) attack vector
- (d) security violation
- (e) attack
- (f) vulnerability
- (g) mechanism

Consider a simple security policy for a house: no one is allowed in the house unless accompanied by a family member, and only family members are authorized to remove physical objects from the house. An unaccompanied stranger in the house is a(n) ..... . An unlocked back door is a(n) ..... . A stranger entering through such a door, and removing a television is a(n) ..... , amounts to a(n) ..... . The ..... is entry through the unlocked door. A(n) ..... here is the existence of an individual motivated to profit by stealing an asset and selling it for cash.

**Solution**: a - security violation b - vulnerability c - attacker d - attack e - attack vector f - threat

6 2. Explain how each of the following attacks can occur and briefly differentiate between them:

1. Man-in-the-middle attack
2. Replay attack
3. Mafia attack

Provide a clear explanation for each attack and distinguish between them by highlighting their key differences.

**Solution**: **Man-in-the-middle (MITM) attack**: This attack occurs when an attacker intercepts communication between two parties and can eavesdrop or modify the data being exchanged. The attacker can impersonate one of the parties and fool the other party into providing sensitive information. For example, an attacker can insert themselves between a user and a website, making the user believe they are communicating with the legitimate website while the attacker can steal the user's credentials.

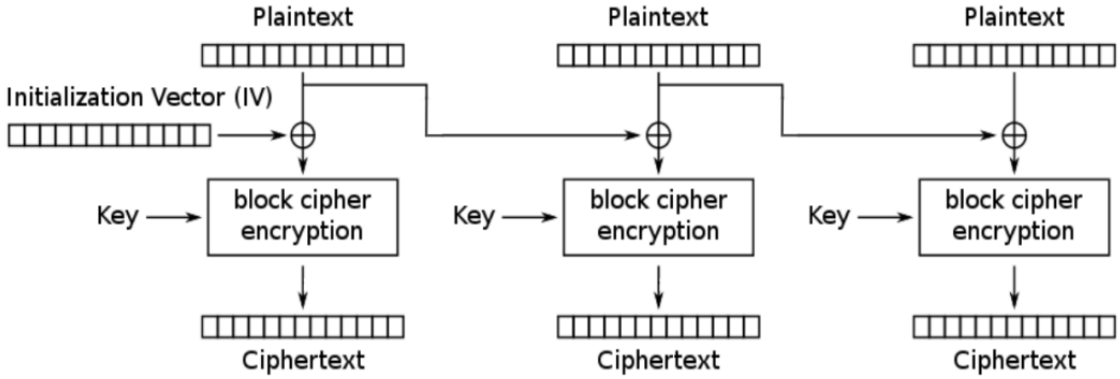
**Replay attack**: This attack occurs when an attacker intercepts and saves the data exchanged between two parties, and then replays that data back to one of the parties at a later time. For example, an attacker can intercept a valid login request and replay it multiple times to gain access to a system.

**Mafia fraud**: In a Mafia fraud attack, also known as grand-chess master fraud, the attacker convinces the victim to contact them and then connects to another service on behalf of the victim. The attacker then uses the victim to confirm the communication with the service, deceiving the victim into unknowingly participating in the attack.

# Q3- Cryptography

12 Consider the following block cipher mode of operation. $M_i$ is the $i$th plaintext block. $C_i$ is the $i$th ciphertext block. $E_K$ is AES encryption with key $K$.
Determine which of the following is true about this scheme? Provide a one-paragraph explanation to support your reasoning.

$$C_0 = M_0 = IV$$
$$C_i = E_K(M_{i-1} \oplus M_i)$$




(a) The encryption algorithm is parallelizable

**Answer:**

(b) If one byte of a plaintext block $M_i$ is changed, then the corresponding ciphertext block $C_i$ will be different in exactly one byte

(b) If one byte of a plaintext block $M_i$ is changed, then the next ciphertext block $C_{i+1}$ will be different in exactly one byte

**Answer:**

(c) If two plaintext blocks are identical, then the corresponding ciphertext blocks are also identical

**Answer:**

(d) The encryption algorithm requires padding the plaintext

**Answer:**

**Solution**:

(a) **True**. By looking at the equation or the diagram, we can see that ciphertext block Ci does not depend on any previous ciphertext block (it only depends on plaintext blocks Mi1 and Mi).

(b) **False**. Since the plaintext block is passed through a block cipher, changing one byte of block cipher input will cause the block cipher output to be completely different.

(b) **False**. Changing one byte of $M_i$ will change one byte of $M_i$ XOR $M_{i+1}$, the input to the block cipher. Again, changing one byte of block cipher input will cause the block cipher output to be completely different.

(c) **False**. Since the plaintext block is XOR'd with the previous block of plaintext before being passed into a block cipher, the corresponding ciphertext blocks are not necessarily identical.

(d) **True**. The plaintext is passed as an input to the block cipher, so it must be padded to a multiple of the block size.

6 2. Explain the differences between Stream Ciphers and Block Ciphers in brief. Your answer should clearly identify the key characteristics that distinguish these two types of encryption algorithms.

**Solution**: Stream Ciphers are encryption algorithms that operate on plaintext one bit at a time and generate a keystream of pseudorandom bits to encrypt the plaintext. The keystream is generated using a key and an initialization vector (IV). Unlike Block Ciphers, Stream Ciphers do not divide the message into blocks and they are not secure against brute-force attacks as the key has a fixed length.
On the other hand, Block Ciphers are encryption algorithms that divide the plaintext message into fixed-length blocks and encrypt them one at a time. Each block is encrypted using the same key and produces a ciphertext block. Block Ciphers can use various modes of operation to add more security and randomness to the encryption process, such as Cipher Block Chaining (CBC) or Electronic Codebook (ECB) modes.

# Q4 - Hash Function

6 1. List at least three common applications of hash functions.

**Solution**: Unique Digests, Public-key Signatures, Chained Hash, Commitment, Checksums (Integrity)

# Q5 - Authentication

6 1. Define the terms Authentication, Identification, and Authorization, and provide a brief explanation of each term. Be sure to differentiate between these terms and give examples of how they are used in security domain.

**Solution**: Authentication: process of using supporting evidence to corroborate an asserted identity Identification (recognition): establish identity from available information (without assertion) Authorization: determining if a request should be granted based on an entity

# Q6 - Certificates

You are working as a software engineer for an online discussion forum called Piazzzzza, which uses the following certificate hierarchy:

1. Everyone has access to the public key of a trusted root certificate authority (CA)
2. The root CA uses its private key to sign a certificate C for Piazzzzza's public key
3. Piazzzzza uses its private key to sign a certificate for each user's public key

Indicate whether the following statements are true or false. Explain why?

4 1. An attacker who steals the private key of the root CA can forge C.

**Solution**: True. The attacker can use the private key of the root CA to sign a fake certificate C.

4 2. An attacker who steals the private key of Piazzzzza can forge C.

**Solution**: False. C is signed by the root CA's private key. The attacker cannot use Piazzzzza's private key to sign C.

4 3. An attacker who steals the private key of a user can forge C.

**Solution**: False. As in the previous part, C is signed by the root CA's private key. The attacker cannot use the user's private key to sign C.

8 4. Compare and contrast the benefits of Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs). In your answer, explain what OCSP provides that CRLs do not.

**Solution**: OCSP and CRLs are both methods used to check the revocation status of digital certificates.
A CRL is a list of revoked certificates that is distributed by the Certificate Authority (CA). When a user needs to verify a certificate, they can download the CRL and check if the certificate is on the list. CRLs have the advantage of being simple and easy to implement, as they only require downloading and parsing a list. However, CRLs can become quite large, as they contain all revoked certificates, and may not be updated frequently.
OCSP provides a more efficient and secure method for checking the revocation status of digital certificates. With OCSP, the user sends a request to the CA asking if a specific certificate is still valid. The CA then sends a signed response indicating the status of the certificate. OCSP has the advantage of being faster than CRLs, as it only requires a single request and response for each certificate. Additionally, OCSP responses can be more granular than CRLs, as they can indicate the status of a single certificate rather than requiring a full list.

*** THE END ***